SB 220 – Cybersecurity safe harbor
Testimony by Curtis Fifner
For the Ohio Association for Justice
Before the Senate Government Accountability & Reform Committee
January 31, 2018

Chairman Coley, Vice Chairman Uecker, Ranking Member Schiavoni and members,

Thank you for the opportunity to provide opponent testimony on Senate Bill 220. My name is Curtis Fifner. I am a trial lawyer and a member of the Ohio Association for Justice, the state bar association for attorneys who help people get back on their feet financially after they have been injured in a car collision or in the workplace, by a defective product, or as a result of a medical error, or those who have been damaged because their identities have been stolen in a data breach.

I want to begin, Mr. Chairman, by acknowledging there is value in encouraging businesses to do the right thing and implement cybersecurity protections. We appreciate the intentions behind SB 220 and don't want our testimony to be interpreted as a rejection of their well-meant objective.

The question is: Will this special legal protection work as intended?

Will a business executive who has decided not to spend the money to implement cybersecurity … or who doesn't have the time as he or she races from project to project, trying to drum up orders, and meet payroll … will a state law establishing an affirmative defense to legal claims serve as the tipping point that causes a business executive to implement cybersecurity protection? We doubt it.

I'd like to set the record straight on the contention that if the affirmative defense proposed in SB 220 is enacted, there will still be a legal basis to file claims for individuals and small businesses that suffer damages from a breach. An affirmative defense is meant to defeat or mitigate the legal consequences of a defendant's otherwise unlawful conduct. It would be used to thwart any viable claim no matter how negligent or reckless, or even how willful and wanton, the conduct was that allowed the breach to occur. In short, it will be very difficult for people that suffer damages to succeed with a legal claim under state law.

At the heart of this proposal is an incentive, an affirmative defense against legal claims, that will be attach to any business entity that complies with the NIST cybersecurity

framework (NIST stands for National Institute of Standards and Technologies under the US Department of Commerce) "or other industry cybersecurity framework," as defined in 1343.03 (starting in line 73). But the legislation doesn't even require full compliance. It says the compliance shall be deemed, and the affirmative defense shall attach, if an entity "is in substantial compliance" (see Sec 1354.03 starting in line 73). Obviously, the term "substantial" will be the subject of litigation for years to come.

Based on our cursory research, compliance with the NIST cybersecurity framework is too easy, in the opinion of some experts, and may be too relaxed a standard to be considered as a fair trade-off for the special legal protections afforded in this legislation. Critics of NIST are quoted as saying: "Compliance with the NIST CSF only requires adopting the terminology. If you speak in those terms and talk in those terms you can be compliant with the framework without changing anything you have to do. It's really a business-friendly framework because it allows the business to decide based on its needs and resources to simply cherry pick what it wants." (*NIST Cybersecurity Framework is Good and Bad, Experts Say*, August 21, 2014: http://www.digitalcrazytown.com/2014/08/nist-cybersecurity-framework-is-good.html)

In combination, the affirmative defense and the substantial compliance phrase won't prevent legal claims from being filed, but it is more likely to increase legal costs. At the outset of litigation, thousands of claims may be filed, mountains of evidence collected, hours of depositions taken, just to determine if the breached corporation was in substantial compliance with NIST and deserves the affirmative defense.

If a damaged party is able to clear the legal hurdle by showing the entity was NOT in substantial compliance, and therefore the affirmative defense does not apply, next the plaintiff has the burden to show the defendant was negligent. Virtually all of these legal actions are brought under state law. Negligence is the primary legal theory most often asserted, followed by actions alleging violations of consumer protection, breach of contract, unjust enrichment and fraud. Only a fraction of these claims are brought under the Federal Stored Communications Act, which is the only cause of action where the federal courts will have jurisdiction.

Past history indicates this bill would excuse from accountability major corporations that are breached. Just 27 defendants faced data breach litigation in 2016. None of these were small companies; all were major corporations. Almost all (89%) involved a breach of sensitive information like Social Security numbers, medical treatment information, and health insurance information. To the best of our knowledge, all of these major corporations that were breached in 2016 were NIST compliant. So if this legislation is enacted, it excuses and defeats all the negligent acts by these companies that caused

millions of people to have their personal information stolen. This leads to fraudulent tax returns, the ability for people to steal identity and credit cards, and even obtain fraudulent concealed carry licenses.

We invite you to take a step back and think through the possible consequences of this legislation. This is a first-of-its kind legislation, not enacted by any other state, so we don't know what the outcomes will be. However, we do know that the bill would serve as a bar to recovery for consumers and small businesses who suffer real damages. And we suspect that the bill would not make a difference in the number of companies that implement cybersecurity protections.

Thank you, Mr. Chairman and members, for listening to our views on SB 220. If you have questions, it would be my pleasure to continue our conversation.